REMARKS

Claims 11- 23 have been cancelled. Claims 1, 5, 7, 24, 29-31, 34 and 37 are proposed to be amended herein. Claims 1-10 and 24-39 are presently pending in the above-identified application.

Rejection of Claims 4 and 5 under 35 USC § 112

The Office action rejected claims 4 and 5 as being indefinite under 35 USC § 112 in view of the use of the terms "compressed" and "decompressing", respectively. Applicants respectfully disagree and point the Examiner's attention to Applicants' Specification, page 14, line 13 through page 15, line 4 which details an alternative embodiment of the instant invention where the cryptographic shares "may be compressed in order to save memory space". One of ordinary skill in the art will readily understand the compression and decompression details with regard to the disclosed alternative embodiment and achieving such data storage (i.e., memory) savings. Applicants respectfully request that this rejection be withdrawn.

Rejection of Claims 1-14, 16, 19-23, 34, 37 and 39 under 35 USC § 102

The Office Action rejected the originally filed claims 1-14, 16, 19-23, 34, 37 and 39 as being anticipated by U.S. Patent No. 5,802,175 issued to S. Kara et al. (hereinafter "Kara"). Applicants have amended the claims herein to more particularly claim the various aspects of the invention, and respectfully submit that each of the currently pending claims is patentably distinct from Kara for at least the reasons set forth hereinbelow.

Amended Independent Claims

More particularly, the present invention provides for the generation of a repeatable cryptographic key based on potentially varying parameters which are received, for example, during a computer resource access attempt. The key is repeatable in that the same key may be generated using different received parameters. In accordance with the invention, so-called cryptographic shares are retrieved from memory locations identified

as a function of the parameters. In particular, in accordance with an aspect of the invention, a function is applied to the parameters in order to generate a set of indices which indices, in turn, are used to access the stored cryptographic shares for generation of the cryptographic key (see, e.g., Applicants' Specification, page 8, line 24 through page 9, line 25; and page 6, lines 15-22). It is at least this aspect of Applicants' invention that stands in contrast to the cited prior art.

Significantly, it is the use of the received parameters (see, e.g., Applicants' Specification, page 6, lines 25-27), once obtained, to generate the indices for accessing the stored cryptographic shares for generating the repeatable cryptographic key that is the subject of the invention. To that end, Applicants have amended the originally filed independent claims to more particularly claim the above-described aspect of the invention. For example, amended independent claims 1 recites:

> "...generating at least one index as a function of said at least one parameter, said one parameter being from a plurality of varying parameters;
>
> retrieving at least one cryptographic share from a memory location identified as a function of said at least one index; and
>
> generating a cryptographic key based on said at least one cryptographic share." (Emphasis added by Applicants)

Each of the currently pending independent claims has been amended in a similar fashion as the above-referenced amended claim 1 to more particularly claim this aspect of the invention.

Applicants respectfully submit that the pending claims herein are patentably distinct from Kara. More particularly, Applicants' understand Kara to teach a system and method in which cryptographic key sets are generated from unique data supplied from a portable memory device and data supplied from a host computer system and, thereafter, the decryption key is stored only on the portable memory device, making such device necessary to decrypt any files encrypted using the corresponding encryption key (see, e.g., Kara, column 2, lines 42-67). Kara's portable memory device is provided for "seeding" an encryption key generation algorithm and for storing the resulting generated

keys. These operations are further detailed with regard to Kara's so-called "Key Generation Program" (see, e.g., Kara, column 3, lines 2-7; and column 6, lines 8-64).

In rejecting the originally filed independent claims, the Office Action relies predominantly on Kara at column 2, lines 42-67. While such cited passage is directed to the generation and storage of encryption/decryption key sets it does not anticipate Applicants invention as claimed in the amended set of claims herein. That is, Applicants find no teaching or suggestion in the cited Kara passage (or any other in Kara) with respect to the aspect of Applicants' invention, as claimed in the currently pending independent claims, directed to the application of a function to the varying parameters in order to generate a set of indices which indices, in turn, are used to access the stored cryptographic shares upon which the cryptographic key is generated.

In view of the foregoing, Applicants respectfully submit that each of the currently pending independent claims, as amended, are patentably distinct from Kara.

Dependent Claims

Regarding the rejection of each of the originally filed dependent claims these claims, as amended, depend ultimately from one of the pending amended independent claims 1, 24 or 34, as the case may be, which Applicants submit are patentably distinct over Kara for the aforesaid reasons. Thus, these dependent claims contain all the limitations of the pending amended independent claims from which they depend, and Applicants respectfully submit that these dependent claims are also patentably distinct over Kara for the aforesaid reasons, as well as other elements these claims add in combination with their base claim. For example, with respect to at least dependent claims 30 and 31, such dependent claims contain further aspects of Applicants' invention directed to defining a particular function (see, e.g., Applicants' Specification, page 18, lines 15-12) which is applied for determining the claimed indices.

Rejection of Claims 15, 18, 24-33 and 35 under 35 USC § 103(a)

The Office Action rejected originally filed claims 15, 18, 24, 26-27, 29-33 and 35 under 35 USC § 103(a) as being unpatentable over Kara in view of U.S. Patent No.

5,557,686 issued to M. Brown et al. (hereinafter "Brown"). Further, the Office Action rejected originally filed claims 25 and 28 as being unpatentable over Kara in view of Brown in further view of U.S. Patent No. 5,625,692 issued to A. Herzberg et al. (hereinafter "Herzberg"). In view of the cancellation of originally filed dependent claims 15 and 18 the aforementioned rejection of such claims is deemed moot.

Regarding the remaining pending dependent claims, as amended herein, Applicants respectfully submit that nothing in Kara, Brown or Herzberg taken alone or in any combination teaches or suggests the various aspects of Applicants' invention as claimed herein.

More particularly, Applicants recognize that the art teaches various password authentication techniques (like Brown) and secret sharing schemes (like Herzberg). See, for example, Applicants' discussion at Applicants' Specification at page 2, lines 16-28 and page 12, line 27 through page 13, line 3, respectively. However, nothing in the Kara/Brown or Kara/Brown/Herzberg combination teaches or suggests the aspect of Applicants' invention, as claimed in the currently pending claims, directed to the application of a function to the varying parameters in order to generate a set of indices which indices, in turn, are used to access the stored cryptographic shares upon which the cryptographic key is generated.

In view of the foregoing, it is respectfully submitted that each of the currently pending claims in the application is in condition for allowance and reconsideration is requested. Favorable action is respectfully requested.

Should the Examiner believe anything further is desirable in order to place the application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Philip L.Bohannon
Bjorn Markus Jakobsson
Fabian Monrose
Michael Kendrick Reiter
Susanne Gudrun Wetzel

By _____
Donald P. Dinella
Attorney for Applicants
Reg. No. 39,961
908-582-8582

Date: March 26, 2004

Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawfords Corner Road
Holmdel, NJ 07733-3030